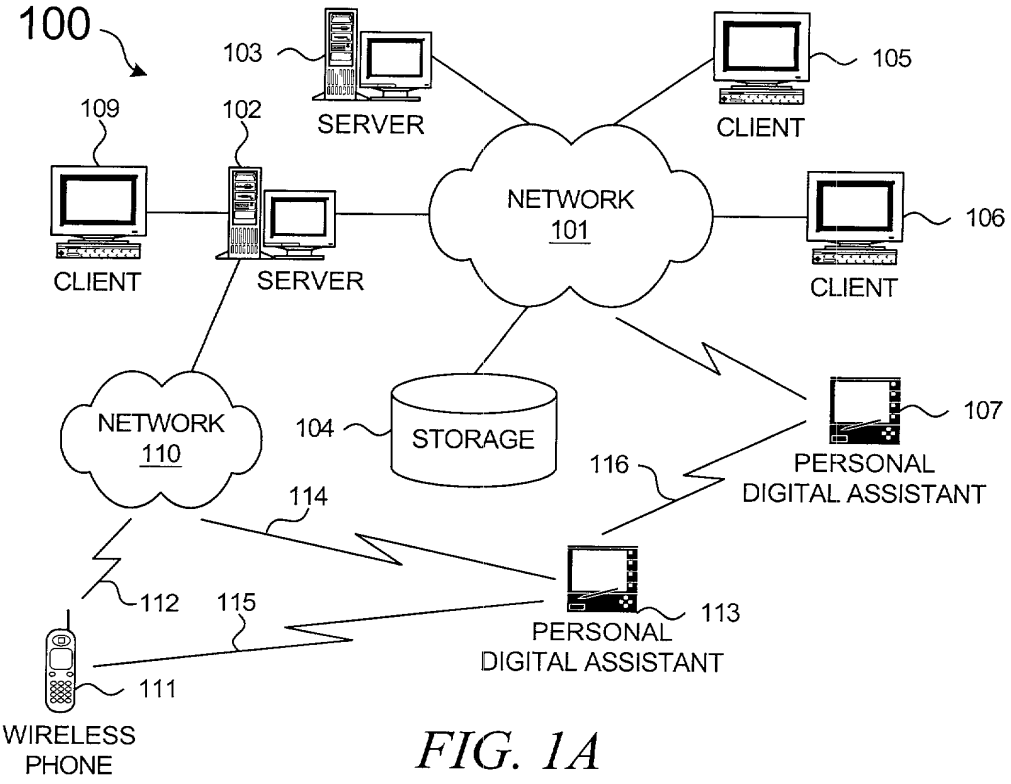

FIG. 1A
(PRIOR ART)

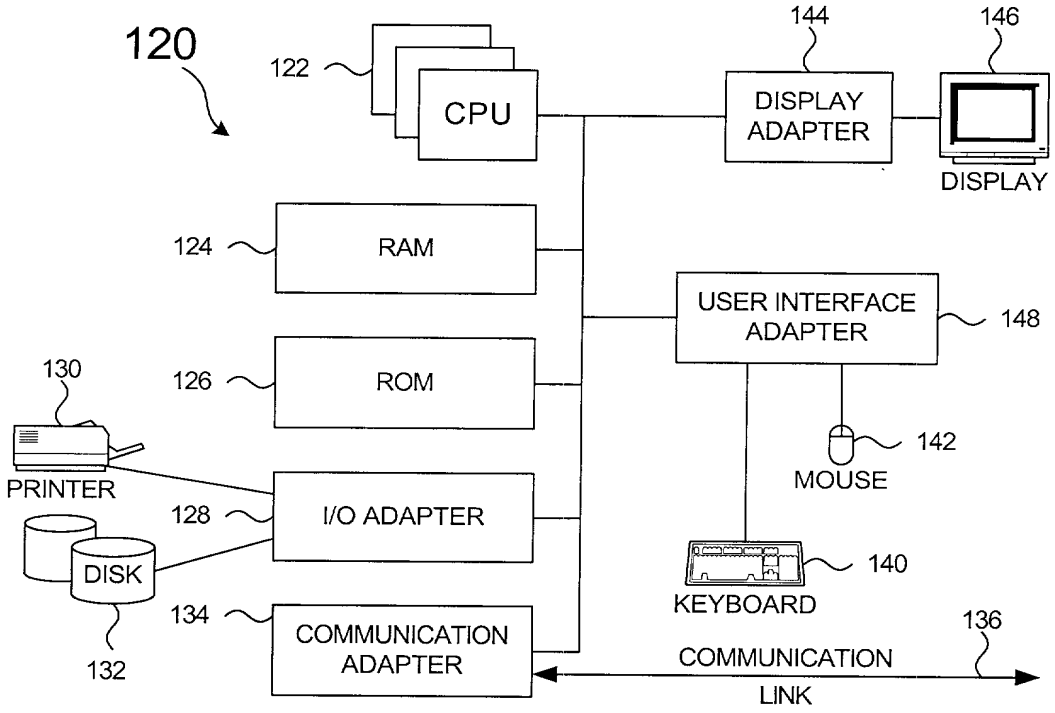

FIG. 1B
(PRIOR ART)

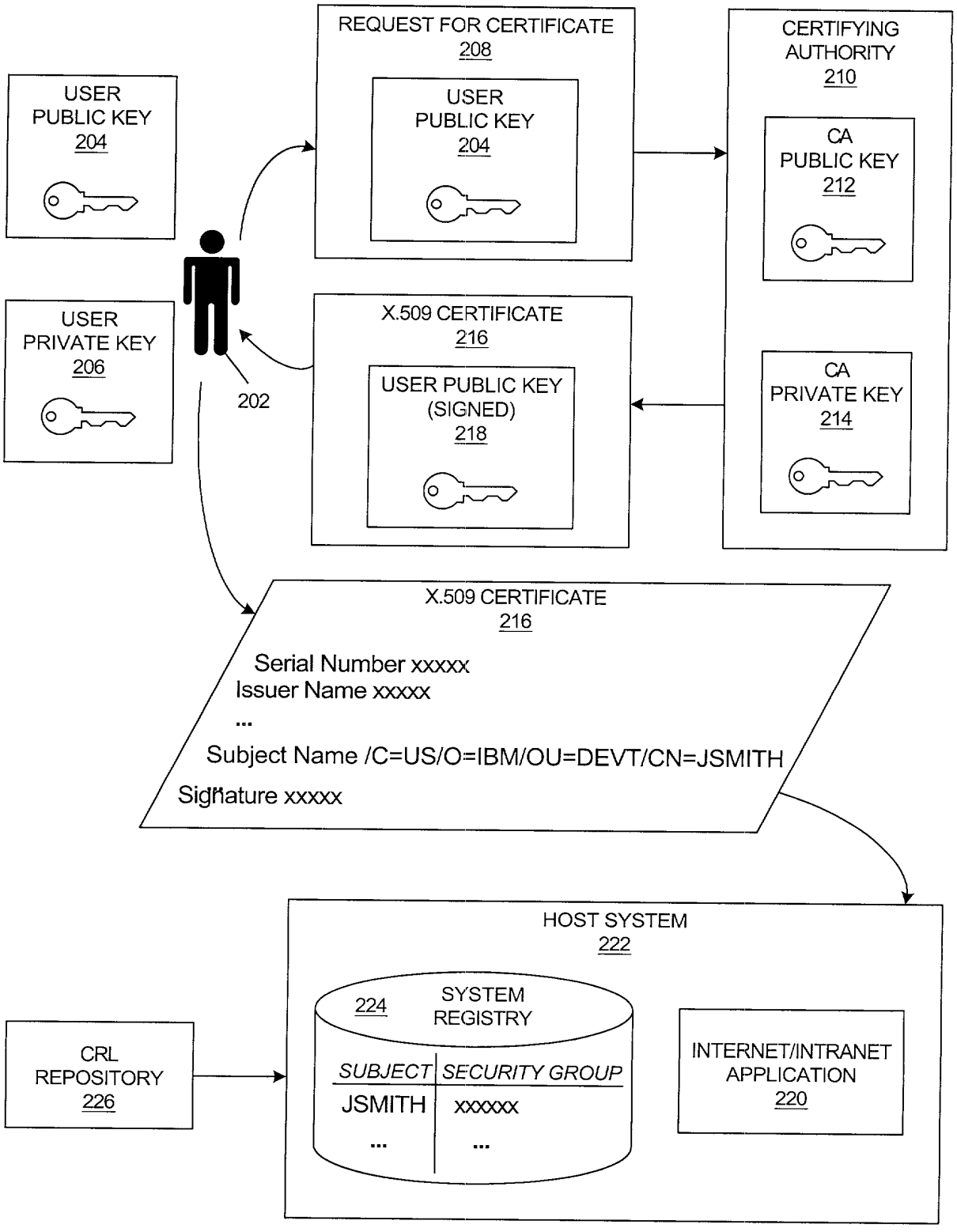

FIG. 2
(PRIOR ART)

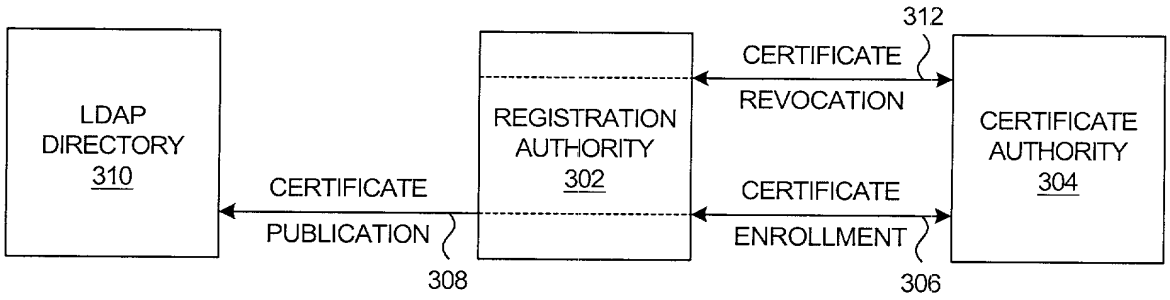

FIG. 3
(PRIOR ART)

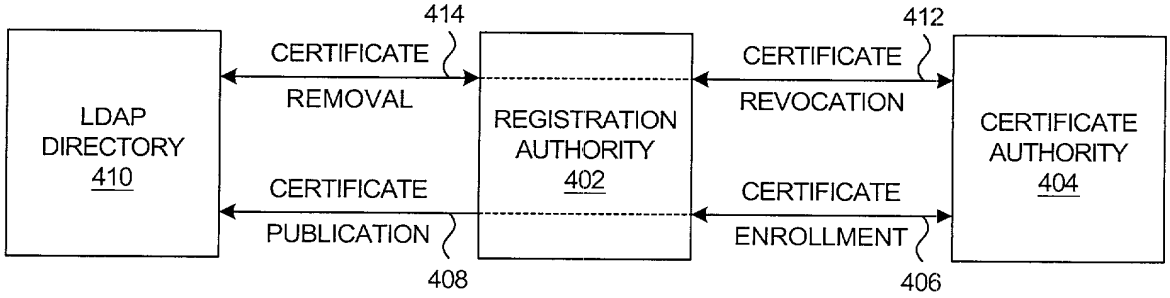

FIG. 4

```
CertificateList  ::=  SEQUENCE  {
      tbsCertList          TBSCertList,
      signatureAlgorithm       AlgorithmIdentifier,
      signatureValue           BIT STRING  }

TBSCertList  ::=  SEQUENCE  {
      version                  Version OPTIONAL,
      signature           AlgorithmIdentifier,
      issuer                   Name,
      thisUpdate          Time,
      nextUpdate          Time OPTIONAL,
      revokedCertificates      SEQUENCE OF SEQUENCE  {
            userCertificate          CertificateSerialNumber,~ 504
            revocationDate           Time,
            crlEntryExtensions       Extensions OPTIONAL
      }  OPTIONAL,
      crlExtensions       [0]   EXPLICIT Extensions OPTIONAL
}
```

FIG. 5B
(PRIOR ART)

```
Certificate  ::=  SEQUENCE  {
      tbsCertificate          TBSCertificate,
      signatureAlgorithm      AlgorithmIdentifier,
      signature               BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
      version           [0]   Version DEFAULT v1,
      serialNumber            CertificateSerialNumber,  ~ 502
      signature               AlgorithmIdentifier,
      issuer                  Name,
      validity                Validity,
      subject                 Name,
      subjectPublicKeyInfo    SubjectPublicKeyInfo,
      issuerUniqueID    [1]   IMPLICIT UniqueIdentifier OPTIONAL,
      subjectUniqueID   [2]   IMPLICIT UniqueIdentifier OPTIONAL,
      extensions        [3]   Extensions OPTIONAL    }

Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
      notBefore               Time,
      notAfter                Time }

Time ::= CHOICE {
      utcTime                 UTCTime,
      generalTime             GeneralizedTime }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
      algorithm               AlgorithmIdentifier,
      subjectPublicKey        BIT STRING  }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
      extnID                  OBJECT IDENTIFIER,
      critical                BOOLEAN DEFAULT FALSE,
      extnValue               OCTET STRING  }
```

FIG. 5A
(PRIOR ART)

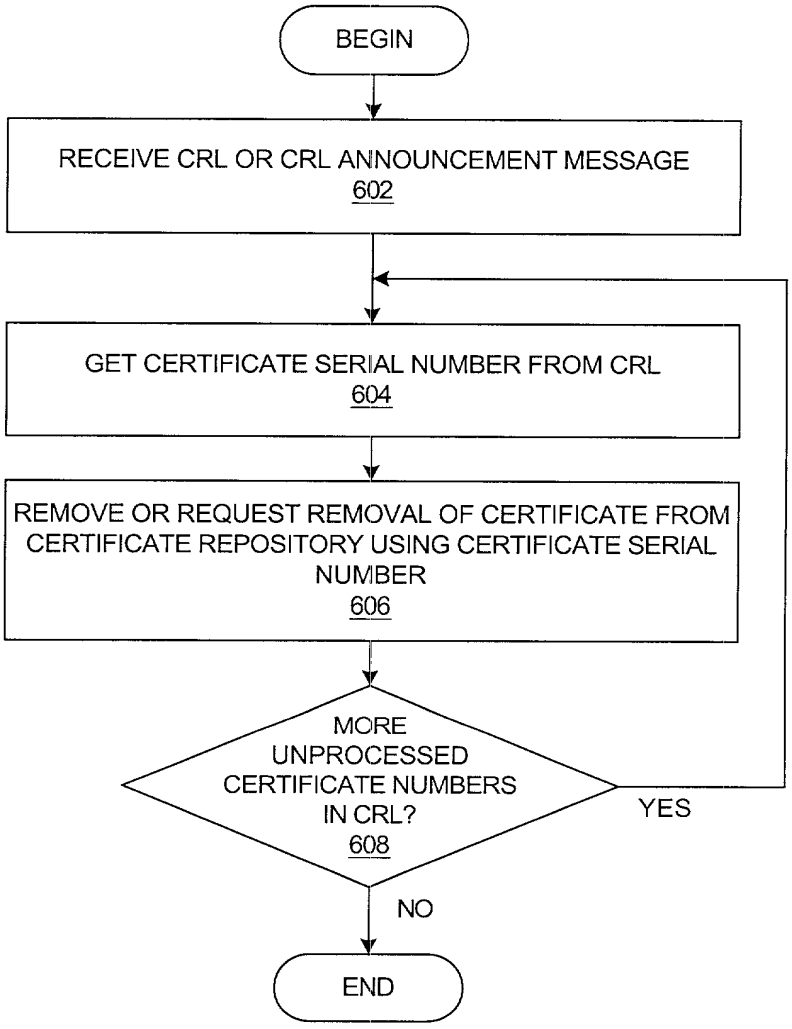
BEGIN
RECEIVE CRL OR CRL ANNOUNCEMENT MESSAGE
602
GET CERTIFICATE SERIAL NUMBER FROM CRL
604
REMOVE OR REQUEST REMOVAL OF CERTIFICATE FROM CERTIFICATE REPOSITORY USING CERTIFICATE SERIAL NUMBER
606
MORE UNPROCESSED CERTIFICATE NUMBERS IN CRL?
608
YES
NO
END

FIG. 6